Listing of the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1: (Canceled)

2: (Previously Presented) The method of claim 7, further including:

the granting service generating a Ticket-Granting-Ticket utilizing a protocol substantially in compliance with the Kerberos protocol; and

wherein receiving by the granting service a request for a Service Ticket from a client further includes the granting service receiving the Ticket-Granting-Ticket from the client.

3: (Previously Presented) The method of claim 7, wherein the granting service determining the number of servers designated to provide the requested service includes:

the granting service utilizing a database that maps a generic server name to a specific server name; and

the granting service setting the numbers of servers designated to provide the service equal to the number of specific server names mapped to the generic server name that provides the requested service.

4: (Previously Presented) The method of claim 3, wherein the granting service utilizing a database that maps a generic server name to a specific server name includes the granting service selecting a database from a group consisting essentially of:

a domain name server database,

a database associated with a Key Distribution Center, and

a Kerberos database.

5: (Original) The method of claim 3, wherein the secret keys associated with each providing server are not synchronized across the providing servers.

6: (Previously Presented) The method of claim 7, wherein the created Service Ticket includes:

a header that designates the Service Ticket as a format that includes multiple encrypted session keys,

a field that expressly designates the number of encrypted session keys,

an encrypted session key for each providing server, and

the encrypted cipher text.

7: (Previously Presented) A method of generating a Service Ticket for a requested Service comprising:

receiving by a granting service of a computing device, the computing device being different and distinct from a client, a request for a Service Ticket from the client;

the granting service determining if the requested service is provided by a plurality of servers:

if not, the granting service generating the Service Ticket utilizing a single server mode; and

if so, the granting service:

generating a session key;

encrypting a cipher text with the session key

determining a number of servers designated to provide the requested service;

for each providing server, encrypting the session key with a secret key associated with each respective server;

creating a Service Ticket that includes an encrypted session key

for each providing server, and the encrypted cipher text; and

transmitting the Service Ticket to the client.

8: (Previously Presented) The method of claim 7, wherein the granting service generating the Service Ticket utilizing a single server mode includes:

the granting service generating a cipher text;

the granting service encrypting the cipher text with a secret key associated with the providing server; and

the granting service transmitting the Service Ticket, that includes the encrypted cipher text, to the client.

9: (Canceled)

10: (Previously Presented) The method of claim 13, wherein the receiving server receiving a Service Ticket is part of a series of client transactions substantially in compliance with the Kerberos protocol.

11: (Previously Presented) The method of claim 13, wherein the receiving server decrypting the encrypted session key includes:

the receiving server determining the number of encrypted session keys included within the received Service Ticket;

for each encrypted session key, the receiving server decrypting the encrypted session key utilizing a secret key associated with the receiving server; and

wherein the receiving server decrypting the cipher text utilizing the decrypted session key includes

for each encrypted session key, the receiving server attempting to decrypt the cipher text with the decrypted session key;

if the cipher text is successfully decrypted, the receiving server providing the service to the client.

12: (Previously Presented) The method of claim 13, wherein the receiving server decrypting the encrypted session key associated with the receiving server utilizing a secret key associated with the receiving server includes:

the receiving server utilizing a server identifier to determine which encrypted session key is associated with the receiving server; and

the receiving server decrypting the associated encrypted session key utilizing a secret key associated with the receiving server.

13: (Previously Presented) A method of authenticating a client's request for a service provided by a service pool comprising:

a server receiving a Service Ticket, the client having at least one encrypted session key, and an encrypted cipher text, the client sending service tickets to multiple severs, including the server, to establish multiple connections;

the receiving server determining if the received Service Ticket includes a plurality of encrypted session keys for multiple servers

if not, the receiving server processing the ticket in a single server mode; and

if so, the receiving server:

decrypting the encrypted session key associated with the receiving server utilizing a secret key associated with the receiving server;

decrypting the cipher text utilizing the decrypted session key; and

providing the service to the client.

14. (Original) The method of claim 13, wherein the receiving server processing the ticket in a single server mode includes the receiving server processing the Service Ticket in utilizing a process substantially compliant with the Kerberos protocol.

15. (Previously Presented) The method of claim 13, wherein the receiving server receiving a Service Ticket includes:

a managing agent first receiving a Service Ticket;

the managing agent selecting the receiving server from a server pool having a plurality of servers;

routing the Service Ticket to the receiving server.

16. (Previously Presented) The method of claim 15, wherein the plurality of servers each includes a secret key associated with the respective servers, and the plurality of secret keys are not synchronized among the plurality of servers..

17. (Original) The method of claim 16, wherein the server pool functions as a group of independent computers working together as a single system.

18 - 33. (Canceled)

34: (Canceled)

35: (Previously Presented) The article of claim 40, further including instructions providing for:

the granting service generating a Ticket-Granting-Ticketing utilizing a protocol substantially in compliance with the Kerberos protocol; and

wherein receiving by the granting service a request for a Service Ticket from a client further includes receiving by the granting service the Ticket-Granting-Ticket from the client.

36: (Previously Presented) The article of claim 40, wherein the instructions providing for the granting service determining the number of servers designated to provide the requested service includes instructions providing for:

the granting service utilizing a database that maps a generic server name

to a specific server name; and

the granting service setting the numbers of servers designated to provide the service equal to the number of specific server names mapped to the generic server name that provides the requested service.

37: (Previously Presented) The article of claim 36, wherein the instructions providing for the granting service utilizing a database that maps a generic server name to a specific server name includes instructions providing for the granting service selecting a database from a group consisting essentially of:

a domain name server database,

a database associated with a Key Distribution Center, and

a Kerberos database.

38: (Original) The article of claim 36, wherein the secret keys associated with each providing server are not synchronized across the providing servers.

39: (Previously Presented) The article of claim 40, wherein the instructions providing for the granting service creating a Service Ticket further includes instructions providing for creating by the granting service a Service Ticket that includes:

a header that designates the Service Ticket as a format that includes multiple encrypted session keys,

a field that expressly designates the number of encrypted session keys,

an encrypted session key for each providing server, and

the encrypted cipher text.

40: (Previously Presented) An article comprising:

a storage medium having a plurality of machine accessible instructions, wherein

when the instructions are executed by a computing device, the instructions provide for:

receiving by a granting service of the computing device, the computing device being different and distinct from a client, a request for a Service Ticket from the client;

the granting service determining if the requested service is provided by a plurality of servers:

if not, generating by the granting service the Service Ticket utilizing a single server mode; and

if so, the granting service:

generating a session key;

encrypting a cipher text with the session key;

determining the number of servers designated to provide the requested service;

for each providing server, encrypting the session key with a secret key associated with each respective server;

creating a Service Ticket that includes an encrypted session key for each providing server, and the encrypted cipher text; and

transmitting the Service Ticket to the client.

41: (Previously Presented) The article of claim 40, wherein the instructions providing for the granting service generating the Service Ticket utilizing a single server mode includes instructions providing for:

the granting service generating a cipher text;

the granting service encrypting the cipher text with a secret key associated with the providing server; and

the granting service transmitting the Service Ticket, that includes the encrypted cipher text, to the client.

42: (Canceled)

43: (Previously Presented) The article of claim 46, wherein the instructions provide for the server receiving a Service Ticket are part of a series of client transactions substantially in compliance with the Kerberos protocol.

44: (Previously Presented) The article of claim 46, wherein the instructions provide for the server decrypting the encrypted session key includes instructions provide for:

the server determining the number of encrypted session keys included within the received Service Ticket;

for each encrypted session key, the server decrypting the encrypted session key utilizing a secret key associated with the receiving server; and wherein decrypting the cipher text utilizing the decrypted session key includes

for each encrypted session key, the server attempting to decrypt the cipher text with the decrypted session key;

if the cipher text is successfully decrypted, the server providing the service to the client.

45: (Previously Presented) The article of claim 46, wherein the instructions provide for the server decrypting the encrypted session key associated with the receiving server utilizing a secret key associated with the receiving server includes instructions provide for:

the server utilizing a server identifier to determine which encrypted session key is associated with the receiving server; and

the server decrypting the associated encrypted session key utilizing a secret key associated with the receiving server.

46: (Previously Presented) An article comprising:

a storage medium having a plurality of machine accessible instructions, wherein when the instructions are executed by a server, the instructions provide for:

the server receiving a Service Ticket, from a client having at least one encrypted session key, and an encrypted cipher text, the client sending service tickets to multiple severs, including the server, to establish multiple connections;

the server determining if the received Service Ticket includes a plurality of encrypted session keys for multiple servers

if not, the server processing the ticket in a single server mode; and

if so, the server:

decrypting the encrypted session key associated with the receiving server utilizing a secret key associated with the receiving server;

decrypting the cipher text utilizing the decrypted session key; and

providing the service to the client.

47. (Previously Presented) The article of claim 46, wherein the instructions provide for the server processing the ticket in a single server mode includes instructions provide for the server processing the Service Ticket in utilizing a process substantially compliant with the Kerberos protocol.

48. (Previously Presented) The article of claim 46, wherein the instructions provide for the server receiving a Service Ticket includes instructions provide for:

a managing agent first receiving a Service Ticket;

the managing agent selecting the server from a server pool having a

plurality of servers;

routing the Service Ticket to the server.

49. (Previously Presented) The article of claim 48, wherein the plurality of servers each includes a secret key associated with the respective servers, and the plurality of secret keys are not synchronized among the plurality of servers..

50. (Original) The article of claim 49, wherein the server pool functions as a group of independent computers working together as a single system.